Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Original) A system for preventing unauthorized access to a network device, comprising:

a headend coupled to a communications network; and

a network device deployed in a home environment and communicatively coupled to the communications network via the headend,

wherein the headend is adapted to determine whether a request to access the network device is authorized.

2. (Original) The system according to claim 1, wherein the headend is adapted to perform at least one of Internet protocol (IP) registration, identification registration and digital rights management.

3. (Original) The system according to claim 1, wherein the headend is adapted to perform at least one of channel/program set up, channel/program management, anonymous proxy services, media caching, media storage, billing and tracking.

4. (Original) The system according to claim 1, wherein the headend is adapted to process at least one of a device identification, an IP address, a digital certificate and a key.

5. (Original) The system according to claim 1, wherein the headend is adapted to store at least one of a device identification, a public key, a hashing signature and an IP address.

6. (Original) The system according to claim 1, wherein the headend is adapted to prevent unauthorized data from reaching the network device.

7. (Original) The system according to claim 6, wherein the data is received by the headend from the communications network.

8. (Original) The system according to claim 1, wherein the headend is adapted to determine whether a particular service provider, which is seeking access to the network device, is authorized to send data to the network device.

9. (Original) The system according to claim 1, wherein the headend is adapted to employ at least one of authentication techniques, encryption techniques and decryption techniques.

10. (Original) The system according to claim 1, wherein the headend is adapted to facilitate pushing a file residing in an authorized device to the network device or to a storage device coupled to the network device.

11. (Original) The system according to claim 10, wherein the pushed file is transported through the headend to the network device or to the storage device coupled to the network device.

12. (Original) The system according to claim 1, further comprising:

a service provider coupled to the communications network and attempting to access the network device via the headend,

wherein the service provider provides at least one of a password or a code to the headend so that the headend can determine whether the service provider is authorized to access the network device.

13. (Original) The system according to claim 1, wherein the network device comprises at least one of a computer, a storage device, set-top box circuitry, a television, a display and a remote control.

14. (Original) The system according to claim 1, wherein the communications network comprises an IP-based communications network.

15. (Original) The system according to claim 1, wherein the headend comprises at least one of a cable headend, a satellite headend and a digital subscriber line (DSL) headend.

16. (Original) The system according to claim 1, wherein the headend is adapted to provide at least some of the functionality of a media exchange server.

17. (Previously Presented) A method for preventing unauthorized access in a communications network, comprising:

(a) receiving, at a headend, a request to access a first device in a home network, the request originating from a second device;

(b) determining, by the headend, whether the second device is authorized to access the first device; and

(c) blocking the second device from accessing the first device if the headend determines that the second device is not authorized to access the first device.

18. (Original) The method according to claim 17, further comprising:

(d) allowing the second device to access the first device if the headend determines that the second device is authorized to access the first device.

19. (Original) The method according to claim 18, wherein allowing the second device to access the first device comprises pushing data onto the first device or onto a storage device coupled to the first device.

20. (Original) The method according to claim 19, wherein pushing data comprises transporting data from the second device, through the headend, and to the first device or to the storage device coupled to the first device.

21. (Previously Presented) A method for preventing unauthorized access in a communications network, comprising:

(a) disposing a headend between a first network device of a home network and a second network device such that a communications path between the second network device and the first network device passes through the headend; and

(b) adapting the headend to determine whether the second device is authorized to access the first device.

22. (Original) The method according to claim 21, further comprising:

(c) blocking the second device from accessing the first device if the second device is determined by the headend not to be authorized to access the first device.

23. (Original) The method according to claim 21, further comprising:

(c) allowing the second device to access the first device if the second device is determined by the headend to be authorized to access the first device.

24. (Original) The method according to claim 21, further comprising:

(c) adapting the headend to provide at least some of the functionality of a media exchange server.

25. (Original) The method according to claim 21, wherein adapting the headend comprises adapting the headend to perform at least one of Internet protocol (IP) registration, identification registration and digital rights management.

26. (Original) The method according to claim 21, wherein adapting the headend comprises adapting the headend to perform at least one of anonymous proxy services, media caching, media storage, billing and tracking.

27. (Original) The method according to claim 21, wherein adapting the headend comprises adapting the headend to process at least one of a device identification, an IP address, a digital certificate and a key.